Goodmans LLP Update

In Force Today: Canadian Privacy Breach Notification and Record Keeping Requirements

As of today, November 1, 2018, Canadian private sector organizations have new legal obligations with respect to reporting and keeping records about privacy breaches. These obligations are summarized below in the form of FAQs, taking into account guidance issued earlier this week by the Privacy Commissioner of Canada.

In what situations must we notify the Privacy Commissioner about a privacy breach?

The requirement to report to the Privacy Commissioner applies where

1. there has been a loss of, unauthorized access to or unauthorized disclosure of personal information resulting from
   a) a breach of an organization's security safeguards or
   b) a failure to establish those safeguards;
2. the personal information is under the organization's control; and
3. it is reasonable in the circumstances to believe the breach creates a real risk of significant harm (RROSH) to an individual.

For the purpose of the RROSH test,

1. "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property; and
2. factors that are relevant to the RROSH analysis include the sensitivity of the personal information involved in the breach of security safeguards (viewed in the totality of its circumstances) and the probability of personal information misuse.

The RROSH analysis guidance from the Privacy Commissioner encourages organizations to develop their own RROSH frameworks, so that breaches are assessed consistently. The Privacy Commissioner also recommends an organization ask the following questions as part of its analysis of the probability of misuse:

- What happened and how likely is it someone would be harmed by the breach?
- Who actually accessed or could have accessed the personal information?
- How long has the personal information been exposed?
- Is there evidence of malicious intent (e.g., theft, hacking)?
- Were a number of pieces of personal information breached, thus raising the risk of misuse?
- Is the breached information in the hands of an individual/entity that represents a reputation risk to the individual(s) in and of itself (e.g., an ex-spouse or a boss depending on specific circumstances)?
- Was the information exposed to limited/known entities who have committed to destroy and not disclose the data?
- Was the information exposed to individuals/entities who have a low likelihood of sharing the information in a way that would cause harm (e.g., in the case of an accidental disclosure to unintended recipients)?
- Was the information exposed to individuals/entities who are unknown or to a large number of individuals, where certain individuals might use or share the information in a way that would cause harm?
- Is the information known to be exposed to entities/individuals who are likely to attempt to cause harm with it (e.g., information thieves)? Has harm materialized (demonstration of misuse)?
- Was the information lost, inappropriately accessed or stolen?
- Has the personal information been recovered?
- Is the personal information adequately encrypted, anonymized or otherwise not easily accessible?

What is the form and content of a breach report to the Privacy Commissioner?

The report to the Privacy Commissioner must be in writing and contain:

1. a description of the circumstances of the breach and, if known, the cause;
2. the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period;
3. a description of the personal information that is the subject of the breach to the extent the information is known;
4. the number of individuals affected by the breach or, if unknown, the approximate number;
5. a description of the steps the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;
6. a description of the steps the organization has taken or intends to take to notify affected individuals of the breach; and
7. the name and contact information of a person who can answer, on behalf of the organization, the Privacy Commissioner's questions about the breach.

The Privacy Commissioner has made available a breach report form at www.priv.gc.ca/media/4844/pipeda_pb_form_e.pdf.

Notably, an organization may submit the best information available at the time of reporting to the Privacy Commissioner and may also make follow-up notifications if it becomes aware of new information.

In what situations must we notify affected individuals?

The requirement to report to affected individuals applies where

1. the report is not otherwise proscribed by law;
2. there has been a loss of, unauthorized access to or unauthorized disclosure of personal information resulting from
   a) a breach of an organization's security safeguards or
   b) a failure to establish those safeguards;
3. the personal information is under the organization's control; and
4. it is reasonable in the circumstances to believe that the breach creates a RROSH to an individual.

What is the form and content of a breach report to individuals?

The notification to an affected individual must contain

1. a description of the circumstances of the breach;
2. the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
3. a description of the personal information that is the subject of the breach to the extent the information is known;
4. a description of the steps the organization has taken to reduce the risk of harm that could result from the breach;
5. a description of the steps affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
6. contact information the affected individual can use to obtain further information about the breach.

What is the timing required for a breach report?

All privacy breach notifications must "be given as soon as feasible after the organization determines that the breach has occurred". This will often require a report before the full facts of the breach are known to the organization, with additional follow-up reports.

How do we notify affected individuals?

The two approaches to sending notification to affected individuals are direct and indirect. Direct notification can be done in person, by telephone, mail, email or "any other form of communication that a reasonable person would consider appropriate in the circumstances". This last form of direct notification allows for flexible forms of notification specific to the circumstances of a particular breach situation. Indirect notification (given by public communication or similar measure that could reasonably be expected to reach the affected individuals) is to be given where

- direct notification would be likely to cause further harm to the affected individual;
- direct notification would be likely to cause undue hardship for the organization; or
- the organization does not have contact information for the affected individual.

Is there anyone else we must notify?

If an organization is required to give notice to an individual, the organization will also have to notify any other organization or government agency of the breach if the notifying organization believes the other organization or government may be able to reduce the risk of harm that could result from the breach or mitigate that harm. This includes law enforcement organizations.

Where an organization has its personal information processed by a third party, which one must report?

In most instances, it is the organization that hires the third party processor that has the reporting obligation. However, in some circumstances, both organizations may be obligated to report a breach. In both situations, it is important for the parties to include in the contract between them provisions that require cooperation and facilitate the recording of breach incidents and any required notification to the Privacy Commissioner and individuals.

With respect to what breaches do we need to keep records, even if there is no RROSH?

An organization is required to keep and maintain a record of ***every*** loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards or from a failure to establish those safeguards, and the personal information that is under the organization's control. Importantly, a record of all such breaches of security safeguards involving personal information will have to be made, not only where there is a real risk of significant harm to an individual.

This is an obligation with a massive scope and many organizations will find they need a new system for privacy incident recordkeeping.

Also importantly, the recordkeeping obligation applies to the organization in control of the personal information, so an organization must include in its contracts with third party processors that they keep, maintain and provide to the organization the required breach records.

What must a breach record contain?

A breach record must contain information that enables the Privacy Commissioner to verify the organization's compliance with the breach notification requirements. In other words, the organization must keep sufficient records to show it is tracking personal information security incidents and properly evaluating the risk of harm to individuals.

The Privacy Commissioner recommends at a minimum a breach record include the date or estimated date of the breach, a general description of the circumstances of the breach, the nature of information involved in the breach, and whether or not the breach was reported to the Privacy Commissioner and affected individuals, as well as perhaps "a brief explanation of why the organization determined there was not a real risk of significant harm in cases where the organization did not report the breach to the Privacy Commissioner and notify individuals".

An organization must provide the Privacy Commissioner with access to, or a copy of, such records upon request.

For how long do we need to keep breach records?

An organization is required to keep and maintain such breach records for a minimum of 24 months after the day on which the organization determines the breach has occurred.

For more information regarding these new requirements, please contact any member of our Privacy Law Group.

Authors

Peter Ruby
pruby@goodmans.ca
416.597.4184

Monique McAlister
mmcalister@goodmans.ca
416.597.4255